中文核心期刊

多用户无源光网络量子密钥分发系统研究

程广明

(中国电子产品可靠性与环境试验研究所 赛宝认证中心,广州 510610)

摘要:提出了量子安全保证的无源光网络(PON)概念,对比分析了独立传输和共纤传输量子无源光网络的特点。设计了基于改进的即插即用系统的多用户无源光网络量子密钥分发(PON-QKD)系统,并对该系统的性能和可行性进行了论证。

关键词:量子密钥分发;无源光网络;波分复用

中图分类号:TN918.91;TN915.9　　**文献标识码**:A　　**文章编号**:1002-5561(2018)01-0005-04

DOI:10.13921/j.cnki.issn1002-5561.2018.01.002

Research on multi-user passive optical network quantum key distribution system

CHENG Guangming

(China Electronic Product Reliability and Environmental Testing Research Institute, CEPREI Certification Body, Guangzhou 510610, China)

Abstract: The concept of passive optical network quantum key distribution (PON-QKD) is put forward, and two schemes of PON-QKD system with independent and shared fiber transmissions are compared. Also, a multi-user PON-QKD system which employs a modified plug-and-play system is proposed. And then the performance and feasibility of this PON-QKD system are analyzed and demonstrated.

Key words: quantum key distribution; passive optical network; wavelength division multiplexing

0 引言

量子密钥分发(Quantum Key Distribution,QKD)是量子通信目前应用最成熟的技术之一,经过最近30多年的发展,QKD取得了很多重要的突破。量子通信网络是QKD迈向规模化应用的必然趋势[1,2]。研究发现,根据QKD网络中间节点的不同,QKD网络可分为3类:基于光学节点的QKD网络、基于信任节点的QKD网络和基于量子中继的QKD网络[3]。基于量子中继的QKD网络可能是未来长距离传输最佳解决方案之一,但遗憾的是目前还处在研究初期,暂不具备实用化的能力。基于信任节点的QKD网络依赖于中间站点的绝对信任,如果网络中的某个节点被劫持,则整个传输链路的安全性难以保障。基于光学节点的QKD网络不需要信任的中间站点,且光学节点设备易于安装和维护,已成为目前QKD网络最常用的形式。基于光学节点的QKD网络可以采用经典光器件作为网络节点,包括分束器、光开光、波分复用器和光纤光栅等[1,4-8]。本文研究基于量子安全保证的无源光网络(PON),设计基于波分复用(WDM)技术的多用户PON-QKD系统。

收稿日期:2017-08-25。

基金项目:国家自然科学基金面上项目(批准号:61572203)资助。

作者简介:程广明(1986-),男,博士,工程师,主要从事量子通信与信息安全方面的研究。

1 量子安全保证的PON

PON一般为树状拓扑结构,一个中心站对应多个光网络单元,下行为广播方式,光分配网络不具备信息寻址功能,原理上每个用户能够接收到光线路终端发送给所有用户的信息。如果有恶意用户取消光网络单位的过滤功能,那么就能获取光线路终端发送给其它用户的信息,并且窃听操作是完全被动的。窃听过程中网络的结构和状态不会出现任何变化,且光线路终端无法自己发现窃听的存在,因此,普通PON的安全性存在很大隐患。

量子保密通信是已经证明可以提供无条件安全

的通信技术，这为 PON 的安全保障提供了一种思路，而且已被实验证明，第一个量子保密通信网络正是基于 PON 结构的[1]，所以基于量子安全保证的 PON 成为可能。

1.1 独立传输量子安全 PON

图 1 为 QKD 与 PON 独立传输的量子安全保证 PON 示意图，光线路终端与每个光网络单元都配置一台 QKD 终端，其中位于光线路终端的 QKD 终端为控制器，能够与多个用户同时通信产生密钥。QKD 网络与 PON 分别拥有各自的光分配网络，分别连接各自网络中的中心站和用户单元，这样网络布置的好处在于两者独立互不影响，但是比较消耗网络资源。当 PON 需要加密通信时，光线路终端和光网络单元分别向 QKD 设备发送量子密钥请求，QKD 设备收到请求后向各自的光线路终端和光网络单元发送量子密钥。光线路终端和光网络单元收到量子密钥后，进行密钥同步处理，如果密钥一致，则同步正确，光线路终端和光网络单元分别用获取的量子密钥对通信数据进行加密和解密；如果密钥不一致，则分别向 QKD 设备重新发送量子密钥请求。

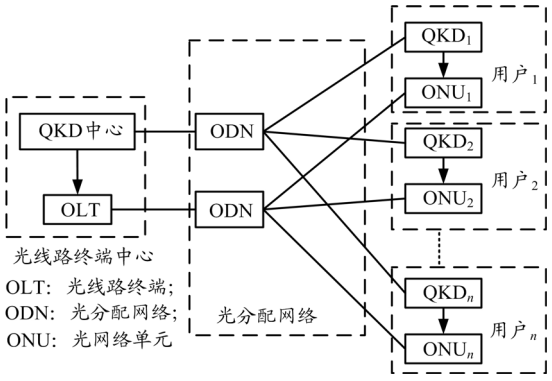


图 1 独立传输的量子安全保证的 PON

1.2 共纤传输量子安全 PON

量子通信与经典通信的共纤传输已经得到多次验证，在 PON 上部署新的量子通信设备，既可以让量子通信充分利用现有的成熟网络设施，又可以利用量子通信增强自身的安全性。图 2 为 QKD 与 PON 共纤传输的量子安全保证的 PON 示意图，与图 1 所示的独立传输线路相比，共纤传输可以节省更多的网络设施。由于共纤传输可能出现信号干扰现象，网络设计时必须考虑 QKD 与 PON 的波长规划，两种波长光信号通过复用器注入到同一根光纤，经过光分配网络的传输，在每个用户单元解复用后被各自的通信终端接收。

2 多用户 WDM–PON–QKD 系统

2.1 方案设计

最早基于分束器的 QKD 网络无法控制光子的路径选择，会出现某个或多个路径轮空而没有通信，这可能浪费一部分光子[1]。为了克服光子分发的随机性，随后出现了用波分复用器代替分束器的多用户 QKD 方案[5]，这种方案较之前方案最大的不同在于每个 Bob 具有不同的波长，复用器能利用波长寻址的方式将不同波长的信号传递给不同的 Bob。由于方案采用的光源为可调谐激光器，虽然单一光源能够产生供与多个 Bob 通信所需的不同波长的激光，但同一时刻只能有一种波长产生，这样仍然无法从根本上克服单用户的密钥生成率受困于用户规模的局面，即随着用户数的增加，单用户的密钥生成率会减小。

为了避免这种密钥生成率随用户增加而减小的低效率情况，我们提出了一种基于改进的即插即用系统的多用户 WDM–PON–QKD 系统，如图 3 所示。Alice 端拥有一个多波长激光器和用于接收返回光子的 4 对单光子探测器。多波长激光器能够产生多个波长的

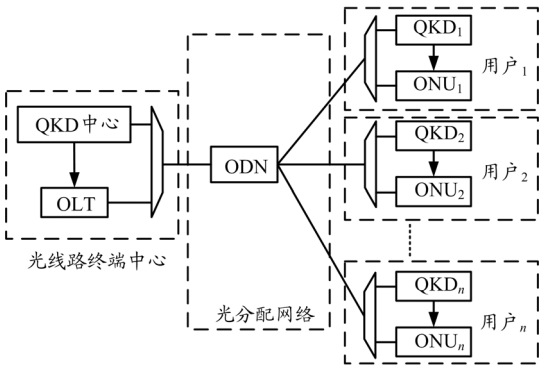


图 2 共纤传输的量子安全保证的 PON

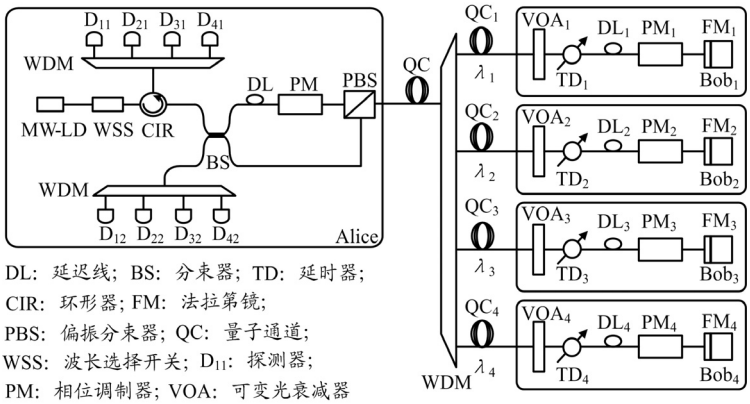


图 3 多用户 WDM–PON–QKD 系统结构

脉冲信号，可利用波长选择开关选择其中 4 个波长脉冲信号并组合成一个脉冲组，作为多用户信息传输的载体。由于各用户相对独立，保证了单用户的密钥生成率稳定，不会随着用户的增加而减小。

2.2 性能分析

筛选密钥速率和量子比特误码率（*QBER*）是衡量 QKD 系统性能的两个重要参数。经理论推导，该 WDM-PON-QKD 系统的筛选密钥速率 R_{sifted} 表示为：

$$R_{\text{sifted}}=\frac{1}{2}f_{\text{rep}}\mu t_{\text{AB}}t_{\text{A}}\eta_{\text{A}}T=\frac{1}{2}f_{\text{rep}}\mu t_{\text{AB}}t_{\text{A}}\eta_{\text{A}}\frac{l_{\text{DL}}}{l_{\text{AB}}+l_{\text{DL}}+t_{\text{DTc}}} \quad (1)$$

其中，f_{rep} 是 Alice 脉冲发射频率，μ 是 Bob 端返回脉冲平均光子数，t_{AB} 是 Alice 与 Bob 间光纤线路的通过率，t_{A} 是 Alice 终端的通过率，η_{A} 是 Alice 端探测器的效率，t_{DT} 是 Bob 端延迟时间，c 是光速，l_{AB} 是 Alice 与 Bob 之间光纤长度，l_{DL} 是 Bob 端延迟线长度。

QBER 代表探测器接收到的错误计数与探测总数之间的比例，该 WDM-PON-QKD 系统的 *QBER* 表示为：

$$QBER=\frac{1-V}{2}+\frac{p_{\text{dark}}}{\mu t_{\text{AB}}t_{\text{A}}\eta_{\text{A}}}+\sum_{n=0}^{n=\frac{1}{p_{\text{det}}}}p_{\text{after}}\left(\tau+n\frac{1}{f_{\text{rep}}}\right) \quad (2)$$

其中，V 是 Alice 端干涉仪的干涉对比度，p_{dark} 是暗计数引起探测器计数的概率，p_{det} 是探测器计数的概率，p_{after} 是后脉冲引起探测器计数的概率。

为了评估 WDM-PON-QKD 系统性能，我们对系统的筛选密钥速率和 *QBER* 进行了数值计算。一般地，Alice 的通过率为 0.6[9]，由于本系统多了解复用器，因此，将其 0.85 的通过率考虑进去，可以得到 Alice 端的通过率为 0.51。其它参数如表 1 所示。

表 1 数值模拟中的部分参数

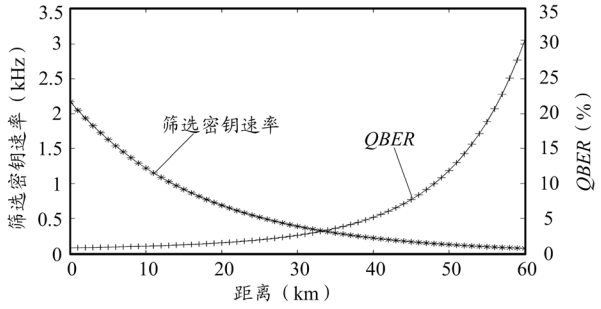
参数	数值
脉冲发射频率（f_{rep}）	5MHz
脉冲宽度	600ps
平均光子数（μ）	0.1
探测器在 1550nm 处的探测效率（η_{A}）	10%
暗计数率（p_{dark}）	10^{-5}/gate
探测器门宽	2.5ns
死时间（τ）	10μs
干涉对比度（V）	99%
后脉冲计数概率（p_{after}）	4.25%
Bob 端延迟线（l_{DL}）	12.5km

图 4 给出了数值模拟的结果。如图 4（a）所示，*QBER* 随着距离的增加呈指数形式增加，而筛选密钥速率呈指数形式下降。在 0~60km 的整个距离范围内，筛选密钥速率下降很快，而 *QBER* 一直维持在比较低的水平，甚至到了 50km，相应的 *QBER* 仍然低于 15%。通常，我们将 *QBER*=15%认为是一个基准线，当 *QBER* 超过 15%时，窃听者能够比合法接收者获得更多的信息，因此此时的结果不能用于下一步的密性放大。图 4(b)对比了考虑时间周期和未考虑时间周期下的筛选密钥速率，在短距离内，两种情况下的筛选密钥速率都保持一个很高的水平，即便二者存在一个明显的差距。但是，当 Bob 端的延迟线长度与 Alice 和 Bob 间距离相近时，脉冲帧发射频率会受到很大程度的限制，最终影响到全局密钥生成率。因此，在不同的环境下，Bob 端的延迟线长度是可调的。

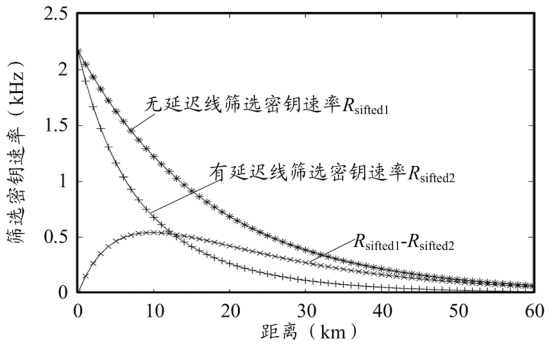
2.3 可行性分析

2.3.1 多信道信号串扰问题

WDM-PON-QKD 系统可行性首要考虑的是多信道信号串扰问题，特别是量子信号与经典信号共纤传输时。为解决此问题，形成了异波段隔离方案[10]和同波段传输方案[11]两类主流方案。由于在自发喇曼散射过程中，反斯托克斯光要远远低于斯托克斯光的强度，为了减少 C 波段经典信号自发喇曼散射对量子信号的影响，前期的研究都将量子信号的波长选在 1310nm



(a) 筛选密钥速率和 *QBER* 随传输距离的变化



(b) Bob 端有无延迟线筛选密钥速率随传输距离的变化

图 4 筛选密钥速率和 *QBER* 数值计算结果

波段，而经典光信号在 1550nm 波段，这种技术称为异波段隔离方案。但是，光纤对 1310nm 波段光的损耗较大，不利于量子信号的长距离传输。为了解决上述问题，同波段传输方案被提出，即量子信号和经典光信号都被分配到 1550nm 波段。不过，同波段的量子信号与经典信号共纤传输会给量子信号带来更大的干扰。为了解决这一干扰，一系列方案被提出，例如波分传输和时分探测方法、滤波器方案、正交频分复用和波段合理分配等。针对本文提出的 WDM-PON-QKD 系统，我们采用波段合理分配的方案。由于量子通信系统的弱信号特点，量子通信网络的波长规划在满足 ITU-T 波长标准的同时，也必须充分考虑四波混频效应。波长规划的一个重要出发点就是要让四波混频产生的新频率光尽可能远离这 4 个脉冲信号的波长。本文利用波长选择开关和采用二级等差频率间隔的方式选择波长，这种适当不等间距的波长信道规划设计，能使产生的新频率光大部分远离其它信号波长，而且四波混频的效率随着波长间隔加大而降低，对系统影响进一步降低。

2.3.2 相位调制的波长相关对 *QBER* 的影响

量子通信系统相位编码的调制器主要为铌酸锂型相位调制器，其相位调制大小除了与相位调制器本身材料和尺寸相关外，还与被调制光信号的波长和调制电压存在直接的关系，这就意味着从 4 个 Bob 返回的光信号同时被同一调制电压调制后仍然会有不同的相位改变。对于不同波长的精确相位调制，通常采用以下两种方法[12]：①精确测量对各波长调制时的不同相位调制电压，当各波长信号通过调制器时，及时加载相应的调制电压。这种方法要求在波长快速变化时，相位调制器的电压必须能够快速进行变化，以便精确地调制到该波长所需的相位。②取中间波长所需相位调制电压为基准调制电压，在调制时，不论哪个波长信号都要采用基准调制电压进行调制。这种方法虽然会引入一定的相位调制偏差，但是不受外部控制系统的性能影响，更易实现高速通信。针对②方法引入的误码率问题，相关文献已经表明[12]，只要光信号波长在一定范围内，即可将采用基准调制电压带来的误码率降低在 1%以内。例如，假设中心波长 λ_c=1550nm，当 $\Delta\lambda=\lambda_n-\lambda_c\leqslant 105$nm 或者 $\Delta\lambda'=\lambda_c-\lambda_n\leqslant 93$nm 时，即 1457nm$\leqslant\lambda_n\leqslant$1655nm，则可以做到 $QBER_{\Delta\Phi}\leqslant 1\%$，对于 93nm 宽的波长间隔，足够本文提出的波分复用 4 个波长信号同时传输。

3 结束语

网络化是量子通信走向大规模应用的必然之路，QKD 网络主要有光学器件、可信中继和量子中继 3 种形式，基于光学器件的 QKD 网络由于结构简单、成本低等原因成为现阶段 QKD 网络实用化部署的主要方式。本文提出了基于量子安全保证的 PON 概念，这为利用并保护 PON 系统提供了一种思考的方向。在此基础上，本文还重点研究了多用户 WDM-PON-QKD 系统，并分析了其性能和可行性。该系统同时利用了 WDM 和 PON 技术，满足多用户同时进行量子通信的需求，希望能对丰富 QKD 网络形式提供有益参考。

参考文献：

[1] TOWNSEND P D. Quantum cryptography on multi-user optical fiber networks[J]. Nature, 1997(385): 47-49.

[2] 徐华彬，周媛媛. 量子网络方案研究[J]. 光通信技术，2017，41(5)：55-58.

[3] 程广明. 量子通信与经典通信网络融合研究 [D]. 广州：华南师范大学，2015.

[4] NISHIOKA T, ISHIZUKA H, HASEGAWA T, et al. "Circular type" quantum key distribution [J]. IEEE Photonics Technology Letters, 2002, 14 (4): 576-578.

[5] BRASSARD G, BUSSIERES F, GODBOUT N, et al. Multiuser quantum key distribution using wavelength division multiplexing [J]. SPIE, 2003(526): 149-153.

[6] TOLIVER P, RUNSER R J, CHAPURAN T E, et al. Experimental investigation of quantum key distribution through transparent optical switch elements[J]. IEEE Photonics Technology Letters, 2003, 15(11): 1669-1671.

[7] KUMAVOR P D, BEAL A C, YELIN S, et al. Comparison of four multi-user quantum key distribution schemes over passive optical networks[J]. Journal of Lightwave Technology, 2005, 23(1): 268-276.

[8] CHENG G, GUO B, ZHANG C, et al. Wavelength division multiplexing quantum key distribution network using a modified plug-and-play system [J]. Optical and Quantum Electronics, 2015, 47(7): 1809-1817.

[9] STUCKI D, GISIN N, GUINNARD O, et al. Quantum key distribution over 67km with a plug&play system[J]. New Journal of Physics, 2002, 4(1): 41.1-41.8.

[10] TOWNSEND P D. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing[J]. Electronics Letters, 1997, 33(3): 188-190.

[11] PETERS N A, TOLIVER P, CHAPURAN T E, et al. Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments [J]. New Journal of Physics, 2009, 11(4): 045012-1-045012-17.

[12] 岳孝林，王金东，魏正军，等. 一种新的单光源多波长双向量子密钥分发系统[J]. 物理学报，2012，61(18)：184215-184217.